REMARKS

Claims 1-23 are pending in the present application. In the Office Action mailed September 19, 2005, maintained the restriction rejection. The Examiner rejected claims 1, 2, 4-10, 18-21, and 23 under 35 U.S.C. §103(a) as being unpatentable over Eveland et al. (USP 6,664,893 – hereinafter Eveland) and Fenstemaker et al (USP 6,490,684 – hereinafter Fenstemaker) and further in view of Houghton et al. (USP 6,009,153 – hereinafter Houghton).

Applicant appreciates the indication that claims 3 and 22 are allowed.

Election/Restriction

In reiterating Applicant's previous statements in support of rejoinder, the Examiner stated that Applicant argued that "Group I and Group II are not patentably distinct." *Office Action, Sep. 19, 2005. p. 2.* This paraphrasing of Applicant's position is inaccurate. Rather, Applicant stated that the Examiner failed to establish that inventions I and II have separate utility. This statement is distinguishable from asserting that "Group I and Group II are not patentably distinct," as the Examiner paraphrased. Applicant seeks reconsideration as outlined below.

The Examiner stated that "Group I (1-10 and 18-23) is directed to *receiving* an activation key from a first location sent to a centralized location and configured to activate an option of a remote device located in a second location." *Id. (emphasis added).* The Examiner also stated that "Group II (11-17) is directed to a centralized location *sending* an activation option to a remote device located remotely from the centralized location." *Id. (emphasis added).* The Examiner then concluded that "Group I and Group II are patentably distinct." *Id.*

While the Examiner's statements with regard to Groups I and II merely paraphrase that called for therein, the Examiner's statement of Group I actually reads on claim 11, which was included in Group II. For example, the Examiner stated that Group I is directed to receiving an activation key from a first location sent to a centralized location. Claim 11 calls for a centralized facility located remotely from an in-field device having an inactive option, and the centralized facility having at least one access computer programmed to request an activation key from a remote secondary support provider. Thus, claim 11 may also be paraphrased as being directed to receiving an activation key from a first location sent to a centralized location. The Examiner further indicated that the activation key is configured to activate an option of a remote device located in a second location. Claim 11 calls for sending a verification script and the activation key from the centralized facility to the in-field device, which, as stated above, is remotely located from the centralized facility, and permit installation of the activation key in the in-field device to

activate the inactive option if the verification script indicates that the in-field device is in condition to activate the inactive option. Thus, claim 11 may also be paraphrased as being directed to an activation key that is configured to activate an option of a remote device located in a second location. Claim 11, therefore, is in both groups, thereby clearly indicating the inappropriateness of restriction.

Similarly, the Examiner's paraphrasing of Group II reads on either claim 1 or claim 18, which are included in Group I. For example, the Examiner stated that Group II is directed to a centralized location sending an activation option to a remote device located remotely from the centralized location. Claim 1 calls for sending an activation key and a verification script, from the centralized facility, to the in-field device at a second location. Claim 18 calls for receiving an activation key from the centralized facility that is uniquely configured by the secondary support vendor to activate the option of the in-field device, the in-field device being located remotely from the centralized facility. Thus, claims 1 and 18 may also be paraphrased as being directed to a centralized location sending an activation option to a remote device located remotely from the centralized location.

Patentability:

The Examiner seems to use inconsistent standards of patentability. That is, the Examiner uses one standard of patentability to make a distinction between Groups I and II, then uses a more stringent standard of patentability to compare the claims to the prior art. The relationship between Groups I and II is much closer than the relationship between the prior art relied on and either Group I or II. For example, claim 1 calls for sending an activation key and a verification script, from a centralized facility, to an in-field device at a second location. Claim 11 calls for sending a verification script and an activation key from a centralized facility to an in-field device. In the rejection of the claims of Group I as discussed below, the Examiner stated, "Examiner is taking to (sic) position that Houghton (sic) request for verification (security password) before transmitting an activation key to the remote device is similar to sending a verification script to the remote device because the request for verification taught by Houghton request (sic) for (sic) verification of the remote device (security password) before an activation key is transmitted to the remote device." *Office Action, supra at p. 4.* Since the prior art fails to teach sending a verification script from a centralized facility to an in-field device, the Examiner must "tak[e] to position" that that taught in Houghton "is similar" to that called for in the claims. The Examiner is, thus, using a different and more stringent standard of patentability between the claims and the prior art than between Groups I and II. Basically, if Groups I and II are, indeed, patentably

distinct, then both groups are patentably distinct over the prior art. The Examiner cannot use inconsistent standards of patentability to fit the need. Therefore, if Group I is patentably distinct from Group II, then Group I and Group II are patentably distinct over the prior art relied on herein.

The Examiner must either allow the claims over the art of record or rejoin all pending claims.

Claim rejections under 35 U.S.C. §103(a)

Nevertheless, a prima facie case of obviousness has not been met by the Examiner in the rejection of claims 1 and 18 under 35 U.S.C. §103(a) as being unpatentable over Eveland and Fenstemaker and further in view of Houghton as discussed below. To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).* The references fail to teach or suggest all the claim limitations of claims 1 and 18.

The Examiner stated that "Eveland teaches . . . receiving, at a centralized facility, an activation key (authorization signal key) sent from a first location (third-party source) and configured to activate an option of an in-field device (medical monitoring device) located in a second location." *Office Action, Sep. 19, 2005, p. 3.* Applicant respectfully disagrees.

Eveland teaches a medical monitoring system that includes a medical monitoring device and a base station. *See col. 3, lines 7-27.* Eveland teaches that the base station communicates with a central unit through a communications link. *Id.* The central unit communicates with third-party sources or databases. *Eveland, col. 3, lines 28-30.* Eveland further teaches that "[t]he medical monitoring device system 52 and the central unit 58 cooperatively determine whether the medical monitoring device 54 may be activated for rendering medical monitoring device service, numeral 26." *Col. 4, lines 20-23.* Eveland teaches a step of obtaining a third-party evaluation that "includes contacting appropriate third-party sources 72." *Col. 4, lines 57-58.* The third-party sources may or may not authorize use of the medical monitoring device by a patient. *See col. 4, line 58 – col. 5, line 15.* Eveland teaches that the final activation decision is typically made at the central unit "because it has the access to the required information in step 26." *Col. 5, lines 27-31.* If the medical monitoring device is to be activated, Eveland teaches that "the central unit 58 issues an activation signal to the medical monitoring device system 52 over the communication link 60 or 62, numeral 34." *Col. 5, lines 32-38.* Thereafter, "[t]he medical monitoring device 54 is activated and enters service, numeral 36." *Id.*

Thus, Eveland teaches a central unit that decides whether a medical monitoring device should be activated. The activation decision includes third-party communications to determine whether the third parties may authorize activation of the medical monitoring device. If the medical monitoring device is to be activated, the central unit issues an activation signal to the medical monitoring device for activation and entering into service.

As stated above, the central unit receives a third-party authorization, but that authorization is not taught or suggested to be the activation key sent to the medical monitoring device as called for in claim 1. That is, claim 1 calls for receiving, at a centralized facility, an activation key sent from a first location and configured to activate an option of an in-field device located in a second location. Claim 1 further calls for sending the activation key and a verification script, from the centralized facility, to the in-field device at the second location. Thus, the activation key received from the first location is sent, along with a verification script, to the in-field device. Eveland does not teach or suggest that the third-party authorization received by the central unit is sent to the medical monitoring device. While the central unit of Eveland may issue an activation signal, Eveland does not teach or suggest that the third-party authorization is that activation signal. Furthermore, neither Fenstemaker nor Houghton teach or suggest receiving, at a centralized facility, an activation key sent from a first location and configured to activate an option of an in-field device located in a second location and sending the activation key and a verification script, from the centralized facility, to the in-field device at the second location.

Claim 18 calls for an in-field device programmed to receive an activation key from a centralized facility that is uniquely configured by a secondary support vendor to activate the option of the in-field device. As stated above, Eveland does not teach or suggest that the third-party authorization communicated to the central unit is an activation key. That is, Eveland does not teach that the third-party authorization is a uniquely configured activation key that is received by the medical monitoring device.

Thus, Eveland fails to teach receiving, at a centralized facility, an activation key sent from a first location and configured to activate an option of an in-field device located in a second location and sending the activation key and a verification script, from the centralized facility, to the in-field device at the second location as called for in claim 1. Further, Eveland fails to teach an in-field device programmed to receive an activation key from a centralized facility that is uniquely configured by a secondary support vendor to activate the option of the in-field device as called for in claim 18.

The Examiner further stated that:

> Houghton specifically teaches a method of remotely located device (server, 10) requesting verification of a security password before a communication signal (activation signal key) is transmitted to a reconfigurable device (fax machine, 5 Houghton, col. 5, lines 1-12) Examiner is taking to (sic) position that Houghton (sic) request for verification (security password) before transmitting an activation key to the remote device is similar to sending a verification script to the remote device because the request for verification taught by Houghton request (sic) for (sic) verification of the remote device (security password) before an activation key is transmitted to the remote device. *Office Action, supra at p. 4.*

Houghton teaches "[a] technique for programming operating parameters in an electronic device, such as programmable configuration settings, us[ing] an interactive response configuration server accessible through the telephone network." *Abstract.* Houghton teaches the generation and transmission of a programming signal that includes a representation of the desired operating parameter settings to a destination device. *See col. 1, lines 61-64.* Houghton further teaches providing "a level of security for the operating parameter programming according to the invention by having the fax machine 5 and/or configuration server 10 perform processes for verifying that the operator attempting to program the fax machine has authority to perform such operation." *Col. 4, line 62 col. 5, line 1.* Houghton also teaches that, "upon establishing a connection between the operator and configuration server 10, the server 10 can request, receive and verify the security password, prior to transmitting the communication signal." *Col. 5, lines 8-11.*

Applicant disagrees with the Examiner that sending a verification script from a centralized facility to an in-field device that generates a report that is sent back to the centralized facility is similar to sending a request for verification or a security password request. Claim 1 calls for sending the activation key and a verification script, from the centralized facility, to the in-field device at the second location and receiving, at the centralized facility, a report generated by the verification script. Such is not taught or suggested in Houghton. While Houghton may teach requesting a security password, Houghton fails to teach or suggest that the security password request generates a report that is received at a centralized facility. That is, Houghton discloses providing a security password to an operator having programming authority and, following a request for verification, the operator inputs a password that is received by the configuration server. *See col. 5, lines 1-11.* As called for in claim 1, the centralized facility receives a report generated by the verification script sent to the in-field device. The request for verification sent by the configuration server of Houghton to the remote device does not generate a

report, which is transmitted to the configuration server as called for in claim 1. Thus, an operator, and not the verification script sent by the configuration server, may input a password communicated to the configuration server.

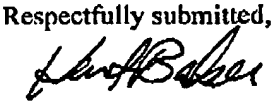
Claim 18 calls for an in-field device programmed to receive a verification script from the centralized facility to authenticate a current status of the in-field device and send a report generated by the verification script to the centralized facility indicating the current status of the in-field device. Similar to that stated above with respect to claim 1, Houghton does not teach or suggest that the password request sent from the configuration server generates a report and sends the report to the configuration server. Further, the password input by the operator and transmitted to the configuration server does not indicate the current status of the in-field device, but rather verifies "that the operator attempting to program the fax machine has the authority to perform such operation." *Col. 4, line 62 – col. 5, line 1.* Neither Houghton nor Eveland nor Fenstemaker teaches or suggests an in-field device programmed to receive a verification script from the centralized facility to authenticate a current status of the in-field device and send a report generated by the verification script to the centralized facility indicating the current status of the in-field device.

Therefore, in light of at least the foregoing, a prima facie obviousness has not been met by the Examiner since the references fail to teach or suggest all the claim limitations of claims 1 and 18. Applicant respectfully believes that the present application is in condition for allowance. As a result, Applicant respectfully requests timely issuance of a Notice of Allowance for claims 1-10 and 18-23.

Applicant appreciates the Examiner's consideration of these Amendments and Remarks and cordially invites the Examiner to call the undersigned, should the Examiner consider any matters unresolved.

Dated: November 21, 2005
Attorney Docket No.: GEMS8081.183

Respectfully submitted,



P.O. ADDRESS:
Ziolkowski Patent Solutions Group, SC
14135 North Cedarburg Road
Mequon, WI 53097-1416
262-376-5170

Kent L. Baker
Registration No. 52,584
Phone 262-376-5170 ext. 15
klb@zpspatents.com